CHAPTER

Domain 2: Asset security

2

CHAPTER OUTLINE

Eleventh Hour CISSP®. http://dx.doi.org/10.1016/B978-0-12-811248-9.00002-4

INTRODUCTION

The Asset Security (Protecting Security of Assets) domain focuses on controls such as data classification, clearances, labels, retention, and ownership of data. We will discuss data remanence, including newly testable material such as the remanence properties of solid-state drives (SSDs), which are a combination of electrically erasable programmable read-only memory (EEPROM) and random-access memory (RAM) and have remanence properties that are quite different in comparison to magnetic drives. The domain wraps up with a discussion of controls determination, including standards, scoping, and tailoring.

CLASSIFYING DATA

The day-to-day management of access control requires management of labels, clearances, formal access approval, and need to know. These formal mechanisms are typically used to protect highly sensitive data, such as government or military data.

LABELS

Objects have labels and subjects have clearances. The object labels used by many world governments are confidential, secret, and top-secret. According to Executive Order 12356—National Security Information:

- “Top Secret” shall be applied to information, of which the unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to national security.
- “Secret” shall be applied to information, of which the unauthorized disclosure could reasonably be expected to cause serious damage to national security.
- “Confidential” shall be applied to information, of which the unauthorized disclosure could reasonably be expected to cause damage to national security.[1]

Private sector companies use labels such as “Internal Use Only” and “Company Proprietary” to categorize information.

CLEARANCE

A *clearance* is a formal determination of whether a user can be trusted with a specific level of information. Clearances must determine the subject's current and potential future trustworthiness; the latter is harder (and more expensive) to assess. Some higher-level clearances include access to compartmented information. *Compartmentalization* is a technical method for enforcing *need to know*.

FORMAL ACCESS APPROVAL

Formal access approval is documented approval from the data owner for a subject to access certain objects, requiring the subject to understand all of the rules and requirements for accessing data, as well as the consequences should the data become lost, destroyed, or compromised.

NEED TO KNOW

Need to know refers to answering the question: does the user “need to know” the specific data they may attempt to access? Most computer systems rely on least privilege and require the users to police themselves by following the set policy and therefore only attempting to obtain access to information of which they have a need to know. Need to know is more granular than least privilege: unlike least privilege, which typically groups objects together, need to know access decisions are based on each individual object.

SENSITIVE INFORMATION/MEDIA SECURITY

Though security and controls related to the people within an enterprise are vitally important, so is having a regimented process for handling sensitive information, including media security. This section discusses concepts that are an important component of a strong overall information security posture.

Sensitive information

All organizations have sensitive information that requires protection, and that sensitive information physically resides on some form of media. In addition to primary storage, backup storage must also be considered. Wherever data exists, there must be processes in place to ensure that the data is not destroyed or inaccessible (breach of availability), disclosed (breach of confidentiality), or altered (breach of integrity).

Handling

People handling sensitive media should be trusted individuals who have been vetted by the organization. They must understand their role in the organization's information security posture. Sensitive media should have strict policies regarding its handling. Policies should require the inclusion of written logs detailing the person responsible for the media. Historically, backup media has posed a significant problem for organizations.

Retention

Media and information have a limited period of usefulness. Retention of sensitive information should not persist beyond this period or legal requirement (whichever is greater), as it needlessly exposes the data to threats of disclosure when the data is no longer needed by the organization. Keep in mind there may be regulatory or other legal reasons that may compel the organization to maintain such data far beyond its time of utility.

OWNERSHIP

Primary information security roles include business or mission owners, data owners, system owners, custodians, and users. Each role has a different set of responsibilities in securing an organization's assets.

BUSINESS OR MISSION OWNERS

Business owners and mission owners (senior management) create the information security program and ensure that it is properly staffed and funded, as well as given appropriate organizational priority. These owners are responsible for ensuring that all organizational assets are protected.

DATA OWNERS

The data owner (also called information owner) is a manager responsible for ensuring that specific data is protected. Data owners determine data sensitivity labels and the frequency of data backup. They focus on the data itself, whether in electronic or paper format. A company with multiple lines of business may have multiple data owners. The data owner performs management duties, while custodians, which will be discussed shortly perform the hands-on protection of data.

SYSTEM OWNER

The system owner is a manager who is responsible for the actual computers that house data. This includes the hardware and software configuration, including updates, patching, etc. The system owners ensure that the hardware is physically secure, operating systems are patched and up to date, the system is hardened, etc. Technical hands-on responsibilities are delegated to custodians, discussed in the next section.

CUSTODIAN

A custodian provides hands-on protection of assets, such as data. They perform data backups and restoration, patch systems, configure antivirus software, etc. The custodians follow detailed orders and do not make critical decisions on how data is protected. The data owner may dictate, “The data owner may dictate that all data must be backed up every 24 h.” The custodians would then deploy and operate a backup solution that meets the data owner's requirements.

USERS

Users must follow the rules; they must comply with mandatory policies, procedures, standards, etc. For example, users must not write their passwords down or share accounts. Users must be made aware of these risks and requirements. They must also be made aware of the penalty for failing to comply with mandatory directives and policies.

DATA CONTROLLERS AND DATA PROCESSORS

Data controllers create and manage sensitive data within an organization. Human resources employees are often data controllers, as they create and manage sensitive data, such as salary and benefit data, reports from employee sanctions, etc.

Data processors manage data on behalf of data controllers. An outsourced payroll company is an example of a data processor. Data processors manage payroll data, which is used to determine the amount to pay individual employees, on behalf of a data controller, such as an HR department.

DATA COLLECTION LIMITATION

Organizations should collect the minimum amount of sensitive information that is required.

The Organisation for Economic Co-operation and Development (OECD) Collection Limitation Principle discusses data limitation: "There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."[2]

MEMORY AND REMANENCE

The 2015 exam update added timely topics such as remanence properties of SSDs, discussed next, followed by a discussion of computer memory itself.

DATA REMANENCE

It is important to understand data remanence when discussing media sanitization and data destruction. Data remanence is data that persists beyond noninvasive means to delete it. Though data remanence is sometimes used specifically to refer to residual data that persists on magnetic storage, remanence concerns go beyond just that of magnetic storage media.

MEMORY

Memory is a series of on/off switches representing bits: 0s (off) and 1s (on). Memory may be chip based, disk based, or tape based. RAM is random-access memory: "random" means the CPU may randomly access or jump to any location in memory. Sequential memory, such as tape, must sequentially read memory, beginning at offset zero, to the desired portion of memory. Volatile memory, such as RAM, loses integrity after a power loss; nonvolatile memory (such as read-only memory (ROM), disk, or tape) maintains integrity without power.

Real or primary memory, such as RAM, is directly accessible by the CPU and is used to hold instructions and data for currently executing processes. Secondary memory, such as disk-based memory, is not directly accessible.

Cache memory

Cache memory is the fastest system memory, required to keep up with the CPU as it fetches and executes instructions. The data most frequently used by the CPU is stored in cache memory. The fastest portion of the CPU cache is the *register* file, which contains multiple registers. Registers are small storage locations used by the CPU to store instructions and data.

The next fastest form of cache memory is Level 1 cache, located on the CPU itself. Finally, Level 2 cache is connected to (but outside of) the CPU. Static random-access memory (SRAM) is used for cache memory.

RAM and ROM

RAM is volatile memory used to hold instructions and data of currently running programs. It loses integrity after loss of power.

ROM is nonvolatile; data stored in ROM maintains integrity after loss of power. A computer *basic input/output system* (BIOS) *firmware* is stored in ROM. While ROM is "read only," some types of ROM may be written to via flashing.

DRAM and SRAM

SRAM is fast, expensive memory that uses small latches called "flip-flops" to store bits. Dynamic random-access Memory (DRAM) stores bits in small capacitors (like small batteries), and is slower and cheaper than SRAM. The capacitors used by DRAM leak charge, and so they must be continually refreshed to maintain integrity, typically every few to a few hundred milliseconds, depending on the type of DRAM. Refreshing reads and writes the bits back to memory. SRAM does not require refreshing and maintains integrity as long as power is supplied.

Firmware

Firmware stores programs that do not change frequently, such as a computer's BIOS (discussed below) or a router's operating system and saved configuration. Various types of ROM chips may store firmware, including programmable read-only memory (PROM), erasable programmable read-only memory (EPROM), and EEPROM, defined next.

PROM can be written to once, typically at the factory. EPROM and EEPROM may be "flashed," or erased and written to multiple times.

A programmable logic device (PLD) is a field-programmable device, which means it is programmed after it leaves the factory. EPROMs, EEPROMs, and flash memory are examples of PLDs.

Flash memory

Flash memory, such as a USB thumb drive, is a specific type of EEPROM that is used for storage. The difference is that any byte of an EEPROM may be written, while flash drives are written by larger sectors.

Solid-state drives

A SSD is a combination of flash memory (EEPROM) and DRAM. Degaussing (destroying data via a strong magnetic field, which we will discuss shortly) has no effect on SSDs. While physical disks have physical blocks (eg, Block 1 is on a specific physical location on a magnetic disk), blocks on SSDs are logical and are mapped to physical blocks. Also, SSDs do not overwrite blocks that contain data; the device will instead write data to an unused block and mark the previous block unallocated.

A process called garbage collection later takes care of these old blocks: "Working in the background, garbage collection systematically identifies which memory cells contain unneeded data and clears the blocks of unneeded data during off-peak times to maintain optimal write speeds during normal operations."[3]

The TRIM command improves garbage collection by more efficiently marking data "invalid" (requiring garbage collection), and skipping data that can be ignored. "TRIM is an attribute of the ATA Data Set Management Command. The TRIM function improves compatibility, endurance, and performance by allowing the drive to do garbage collection in the background. This collection eliminates blocks of data, such as deleted files."[4] While the TRIM command improves performance, it does not reliably destroy data.

A sector-by-sector overwrite behaves very differently on an SSD versus a magnetic drive, and it does not reliably destroy all data. Also, electronically shredding a file (ie, overwriting the file's data before deleting it, which we will discuss shortly) is not effective. Data on SSD drives that are not physically damaged may be securely removed via ATA Secure Erase.

The two valid options for destroying data on SSD drives are ATA Secure Erase and destruction. Destruction is the best method for SSD drives that are physically damaged.

DATA DESTRUCTION

All forms of media should be securely cleaned or destroyed before disposal to prevent *object reuse*, which is the act of recovering information from previously used objects, such as computer files. Objects may be physical, such as paper files in manila folders, or electronic, such as data on a hard drive.

Object reuse attacks range from nontechnical attacks, such as *dumpster diving* (searching for information by rummaging through unsecured trash), to technical attacks, such as recovering information from unallocated blocks on a disk drive.

OVERWRITING

Simply "deleting" a file removes the entry from a file allocation table (FAT) and marks the data blocks as "unallocated." Reformatting a disk destroys the old FAT and replaces it with a new one. In both cases, data itself usually remains and can be recovered through the use of forensic tools. This issue is called *data remanence*, referring to "remnants" of data left behind.

The act of overwriting actually writes over every character of a file or entire disk drive and is far more secure than deleting or formatting a disk drive. Common methods include writing all zeroes or writing random characters. Electronic "*shredding*" or "*wiping*" overwrites the file's data before removing the FAT entry.

DEGAUSSING

Degaussing destroys the integrity of magnetic medium, such as a tape or disk drive, by exposing it to a strong magnetic field, which destroys the integrity of the medium and the data it contains.

DESTRUCTION

Destruction physically destroys the integrity of media by damaging or destroying the media itself, such as the platters of a disk drive. Destructive measures include incineration, pulverizing, and shredding, as well as bathing metal components in acid.

Destroying objects is more secure than overwriting them. It may not be possible to overwrite damaged media, though data may still be recoverable. Highly sensitive data should be degaussed or destroyed, perhaps in addition to overwriting.

SHREDDING

A simple form of media sanitization is shredding, a type of physical destruction. Though this term is sometimes used in relation to overwriting of data, here shredding refers to the process of making unrecoverable any data printed on hard copy or on smaller objects, such as floppy or optical disks.

DETERMINING DATA SECURITY CONTROLS

Determining which data security controls to employ is a critical skill. Standards, scoping, and tailoring are used to choose and customize which controls are employed. Also, the determination of controls will be dictated by whether the data is at rest or in motion.

CERTIFICATION AND ACCREDITATION

Certification means a system has been certified to meet the security requirements of the data owner. Certification considers the system, the security measures taken to protect the system, and the residual risk represented by the system. *Accreditation* is the data owner's acceptance of the certification and of the residual risk, which is required before the system is put into production.

STANDARDS AND CONTROL FRAMEWORKS

A number of standards are available to determine security controls. Some, such as Payment Card Industry Data Security Standard (PCI-DSS), are industry specific; for example, vendors who use credit cards. Others, such as OCTAVE®, ISO 17799/27002, and Control objectives for information and related technology (COBIT), are more general and will be discussed shortly.

PCI-DSS

The PCI-DSS is a security standard created by the Payment Card Industry Security Standards Council. The council is comprised of American Express, Discover, Master Card, Visa, and others. PCI-DSS seeks to protect credit cards by requiring vendors who use them to take specific security precautions.

The core principles of PCI-DSS (available at https://www.pcisecuritystandards.org/security_standards/index.php) are

- Build and Maintain a Secure Network and Systems
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy[5]

OCTAVE®

OCTAVE® stands for *Operationally Critical Threat, Asset, and Vulnerability Evaluation*^{sm}, a risk management framework from Carnegie Mellon University. OCTAVE® describes a three-phase process for managing risk. Phase 1 identifies staff knowledge, assets, and threats. Phase 2 identifies vulnerabilities and evaluates safeguards. Phase 3 conducts the risk analysis and develops the risk mitigation strategy.

The International Common Criteria

The *International Common Criteria* is an internationally agreed-upon standard for describing and testing the security of information technology (IT) products. It presents a hierarchy of requirements for a range of classifications and systems.

CRUNCH TIME

The Common Criteria uses specific terms when defining specific portions of the testing process.

- *Target of evaluation (ToE)*: The system or product that is being evaluated
- *Security target*: The documentation describing the ToE, including the security requirements and operational environment
- *Protection profile*: An independent set of security requirements and objectives for a specific category of products or systems, such as firewalls or intrusion detection systems
- *Evaluation assurance level* (EAL): The evaluation score of the tested product or system

Levels of evaluation

Within the Common Criteria, there are seven EALs, each building upon the previous level. For example, EAL3-rated products can be expected to meet or exceed the requirements of products rated EAL1 or EAL2.

FAST FACTS

The Common Criteria levels are

- EAL1: Functionally tested
- EAL2: Structurally tested
- EAL3: Methodically tested and checked
- EAL4: Methodically designed, tested, and reviewed
- EAL5: Semiformally designed, and tested
- EAL6: Semiformally verified, designed, and tested
- EAL7: Formally verified, designed, and tested[6]

ISO 17799 and the ISO 27000 Series

ISO 17799 was a broad-based approach for the information security code of practice by the International Organization for Standardization, based in Geneva, Switzerland. The full title is *ISO/IEC 17799:2005 Information technology—Security Techniques—Code of Practice for Information Security Management*. ISO 17799:2005 signifies the 2005 version of the standard, based on BS (British Standard) 7799 Part 1.

ISO 17799 had 11 areas, focusing on specific information security controls:

1. Policy
2. Organization of information security
3. Asset management
4. Human resources security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Information systems acquisition, development, and maintenance
9. Information security incident management
10. Business continuity management
11. Compliance[7]

ISO 17799 was renumbered to ISO 27002 in 2005 in order to make it consistent with the 27000 series of ISO security standards. ISO 27001 is a related standard, formally called *ISO/IEC 27001:2005 Information technology—Security techniques—Information Security Management Systems—Requirements*. ISO 27001 was based on BS 7799 Part 2.

COBIT

COBIT is a control framework for employing information security governance best practices within an organization. COBIT was developed by the ISACA (Information Systems Audit and Control Association, see http://www.isaca.org).

COBIT has four domains: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. There are 34 IT processes across the 4 domains. More information about COBIT is available at: http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx. Version 5 was released in Apr. 2012.

ITIL®

ITIL® (Information Technology Infrastructure Library) is a framework for providing best services in IT Service Management. More information about ITIL® is available at: http://www.itil-officialsite.com.

ITIL® contains five *Service Management Practices—Core Guidance* publications:

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement

Service Strategy helps IT provide services. Service Design details the infrastructure and architecture required to deliver IT services. Service Transition describes taking new projects and making them operational. Service Operation covers IT operations controls. Finally, Continual Service Improvement describes ways to improve existing IT services.

SCOPING AND TAILORING

Scoping is the process of determining which portions of a standard will be employed by an organization. For example, an organization that does not employ wireless equipment may declare the wireless provisions of a standard are out of scope and therefore do not apply.

Tailoring is the process of customizing a standard for an organization. It begins with controls selection, continues with scoping, and finishes with the application of compensating controls.

PROTECTING DATA IN MOTION AND DATA AT REST

Data at rest is stored data that resides on a disk and/or in a file. Data in motion is data that is being transferred across a network. Each form of data requires different controls for protection, which we will discuss next.

Drive and tape encryption

Drive and tape encryption protect data at rest and is one of the few controls that will protect data after physical security has been breached. These controls are recommended for all mobile devices and media containing sensitive information that may physically leave a site or security zone.

Whole-disk encryption of mobile device hard drives is recommended. Partially encrypted solutions, such as encrypted file folders or partitions, often risk exposing sensitive data stored in temporary files, unallocated space, swap space, etc.

Media storage and transportation

All sensitive backup data should be stored offsite, whether transmitted offsite via networks or physically moved as backup media. Sites using backup media should follow strict procedures for rotating media offsite.

Always use a bonded and insured company for offsite media storage. The company should employ secure vehicles and store media at a secure site. Ensure that the storage site is unlikely to be impacted by the same disaster that may strike the primary site, such as a flood, earthquake, or fire. Never use informal practices, such as storing backup media at employees' houses.

Protecting data in motion

Data in motion is best protected via standards-based end-to-end encryption, such as IPsec VPN. This includes data sent over untrusted networks such as the Internet, but VPNs may also be used as an additional defense-in-depth measure on internal networks like a private corporate WAN or private circuits like T1s leased from a service provider.

SUMMARY OF EXAM OBJECTIVES

We described the concept of data classification, in use for millennia. We discussed the roles required to protect data, including business or mission owners, data owners, system owners, custodians, and users.

An understanding of the remanence properties of volatile and nonvolatile memory and storage media are critical security concepts to master. We discussed RAM, ROM, types of PROMs, flash memory, and SSDs, including remanence properties and secure destruction methods. Finally, we discussed well-known standards, including PCI-DSS and the ISO 27000 series, as well as standards processes including scoping and tailoring.

TOP FIVE TOUGHEST QUESTIONS

1. A company outsources payroll services to a third-party company. Which of the following roles most likely applies to the third-party payroll company?

A. Data controller

B. Data hander

   - **C.** Data owner
   - **D.** Data processor

2. Which managerial role is responsible for the actual computers that house data, including the security of hardware and software configurations?
   - **A.** Custodian
   - **B.** Data owner
   - **C.** Mission owner
   - **D.** System owner
3. What method destroys the integrity of magnetic media, such as tapes or disk drives, and the data they contain by exposing them to a strong magnetic field?
   - **A.** Bit-level overwrite
   - **B.** Degaussing
   - **C.** Destruction
   - **D.** Shredding
4. What type of relatively expensive and fast memory uses small latches called "flip-flops" to store bits?
   - **A.** DRAM
   - **B.** EPROM
   - **C.** SRAM
   - **D.** SSD
5. What type of memory stores bits in small capacitors (like small batteries)?
   - **A.** DRAM
   - **B.** EPROM
   - **C.** SRAM
   - **D.** SSD

ANSWERS

1. Correct answer and explanation: D. A third-party payroll company is an example of a data processor.
   Incorrect answers and explanations: Answers A, B, and C are incorrect.
   A data controller is someone who creates PII, such as an HR department. "Data handler" is not a formal term and is a distractor answer. A data owner is a management employee responsible for assuring that specific data is protected.
2. Correct answer and explanation: D. A system owner is responsible for the actual computers that house data, including the security of hardware and software configurations.
   Incorrect answers and explanations: Answers A, B, and C are incorrect.
   A custodian is a nonmanager who provides hands-on protection of assets. A data owner is a manager responsible for assuring that specific data is protected. A mission owner is a member of senior management who creates the information

security program and ensures that it is properly staffed and funded and has the appropriate organizational priority.

3. Correct answer and explanation: B. Degaussing destroys the integrity of magnetic media, such as tapes or disk drives, and the data they contain by exposing them to a strong magnetic field.
   Incorrect answers and explanations: Answers A, C, and D are incorrect. A bit-level overwrite removes data by overwriting every sector of a disk. Destruction physically destroys data; for example, via incineration. Shredding electronic data involves overwriting a file's contents before deleting the file.
4. Correct answer and explanation: C. SRAM is relatively expensive and fast memory that uses small latches called "flip-flops" to store bits.
   Incorrect answers and explanations: Answers A, B, and D are incorrect. DRAM is relatively inexpensive memory that uses capacitors. EPROM may be erased with ultraviolet light. A SSD is a combination of DRAM and EEPROM.
5. Correct answer and explanation: A. DRAM stores bits in small capacitors (like small batteries).
   Incorrect answers and explanations: Answers B, C, and D are incorrect. EPROM may be erased with ultraviolet light. SRAM is relatively expensive and fast memory that uses small latches called "flip-flops" to store bits. A SSD is a combination of DRAM and EEPROM.

ENDNOTES

1. *Executive Order 12356—National security information*. http://www.archives.gov/federal-register/codification/executive-order/12356.html [accessed 25.04.16].
2. *OECD privacy principles*. http://oecdprivacy.org/ [accessed 25.04.16].
3. *SSD garbage collection briefly explained*. http://www.ryli.net/ssd-garbage-collection-briefly-explained/ [accessed 25.04.16].
4. *What is TRIM*? http://www.intel.com/support/ssdc/hpssd/sb/CS-031242.htm?wapkw=(TRIM) [accessed 25.04.16].
5. *Payment Card Industry (PCI) Data Security Standard requirements and security assessment procedures (Version 3.1)*. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf [accessed 25.04.16].
6. *Common Criteria (ISO/IEC 15408) certification*. http://www.kyoceradocumentsolutions.com/security/cc.html [accessed 25.04.16].
7. ISO/IEC 17799:2005 http://www.iso.org/iso/catalogue_detail?csnumber=39612 [accessed 25.04.16].